CLAIM AMENDMENTS

IN THE CLAIMS

This listing of the claims will replace all prior versions, and listing, of claims in the application or previous response to office action:

1. (Previously Presented) A computer system comprising:

a processor;

an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;

an input device capable of being coupled to the processor, the input device being adapted to receive a security code, the security code confirming authorized use of the access token;

a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:

an executable program code that accesses the access token and the security code;

an executable program code that verifies validity of the access token by comparing the security code to a verification data on the access token, whereby if the security code matches verification data the access token is valid;

an executable program code that receives a set of security policies from the access token in the processor if the access token is valid; and

an executable program code that controls access to resources in the processor based on the security policies.

2. (Previously Presented) The computer system of claim 1 further comprising:

a nonvolatile storage device operably coupled to the processor;

a nonvolatile storage device access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the executable program code verifying that the security code matches the verification data on the access token.

3. (Previously Presented) The computer system of claim 2, wherein at least one of the set of security policies is stored within the nonvolatile storage device password.

4. (Previously Presented) The computer system of claim 1, wherein at least one of the set of security policies is stored on the access token.

5. (Previously Presented) The computer system of claim 1 wherein one of the set of security policies corresponds to the verification data.

6. (Previously Presented) A computer system comprising:

a processor;

an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;

an input device capable of being coupled to the processor, the input device being adapted to receive verification data, the verification data confirming authorized use of the access token;

a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:

an executable program code that accesses the access token and the verification data;

an executable program code that verifies validity of the access token using the verification data;

an executable program code that sets security policies in the processor, wherein one of the one or more policies includes a BIOS control information that is used to configure the computer system; and

an executable program code that controls access to resources in the processor based on the security policies.

7. (Previously Presented) The computer system of claim 6 wherein the BIOS control information further includes password change information, the password change information including one or more password change settings for a user using the one or more security policies.

8. (Previously Presented) A computer system comprising:

a processor;

an access token communicator capable of being coupled to the processor, the access token communicator being adapted to read an access token;

an input device capable of being coupled to the processor, the input device being adapted to receive verification data, the verification data confirming authorized use of the access token;

a software system executable on the processor and including a system security process controlling operational access to the processor, the software system including:

an executable program code that accesses the access token and the verification data;

an executable program code that verifies validity of the access token using the verification data;

an executable program code that sets security policies in the processor;

an executable program code that controls access to resources in the processor based on the security policies; and

a display device, wherein one of the one or more security policies includes one or more interface settings that control a desktop presentation on the display device.

9. (Original) The computer system of claim 2 wherein a password corresponding to the nonvolatile storage device access password is stored on the access token.

10. (Original) The computer system of claim 2 wherein one or more bytes of the nonvolatile storage device access password are in a non-keyboard enterable format.

11. (Original) The computer system of claim 1 wherein the access token includes one or more bytes of data in a non-keyboard enterable format.

12. (Original) The computer system of claim 1 wherein the verification data includes biometric data supplied by a user.

13. The computer system of claim 1 wherein the input device includes a keyboard and the verification data includes a personal identification number.

14. (Cancelled).

15. (Previously Presented) A computer system comprising:

one or more processors;

memory electrically interconnected to the one or more processors;

an operating system for controlling the operation of the one or more processors;

an access token communication device electrically interconnected to at least one of the one or more processors, the access token communication device being communicatively operable with an access token;

an input device electrically interconnected to at least one of the one or more processors, the input device operable to transmit a security code from a user to the one or more processors;

a nonvolatile storage device electrically interconnected to at least one of the one or more processors, the nonvolatile storage device including a nonvolatile memory;

a set of security policies associated with the operating system, the operating system operable to receive the security code for selectively enabling the set of security policies to limit access to the computer system; and

the operating system permitting access to the nonvolatile storage device and the one or more processors if the security code and the set of security policies match an authorization data stored in the nonvolatile memory,

wherein the access token further includes verification data, the verification data operable to provide the security policies to the nonvolatile memory if the security code matches an authentication code stored in the access token.

16. (Previously Presented) The computer system of claim 15 wherein the operating system includes a BIOS and the BIOS is stored in the nonvolatile memory that is electrically interconnected to the one or more processors.

17. (Previously Presented) The computer system of claim 15 wherein the access token communication device includes a smart card communication device.

18. (Previously Presented) The computer system of claim 15 wherein the access token communication device includes network circuitry that is adapted to receive signals from one or more computers interconnected on a computer network.

19. (Previously Presented) The computer system of claim 15 wherein the access token communication device includes a modem that receives signals from a communications line.

20. (Previously Presented) The computer system of claim 15 wherein the input device is a keyboard.

21. (Previously Presented) The computer system of claim 15 wherein the input device includes a biometric data reading device.

22. (Previously Presented) The computer system of claim 15 wherein the biometric data reading device includes a fingerprint scanner.

23. (Previously Presented) The computer system of claim 15 wherein the biometric data reading device includes a retinal scanning device.

24. (Previously Presented) The computer system of claim 15 wherein the nonvolatile storage device includes a hard disk drive.

25. (Previously Presented) The computer system of claim 15 further comprising a data access code stored in the nonvolatile memory, wherein a data request code corresponding to the data access code alters a state of the nonvolatile storage device.

26. (Previously Presented) A method for accessing a computer system, said method comprising:

providing a computer system, the computer system including:

one or more processors;

a memory operably coupled to the one or more processors;

an operating system for controlling the operation of the one or more processors;

an access token reading device that is adapted to read information stored on an access token;

an input device that is adapted to transmit verification data to the operating system, the verification data confirming authorized use of the access token;

a nonvolatile storage device operably coupled to the memory;

a nonvolatile storage device access password that selectively allows access to the nonvolatile storage device, wherein the nonvolatile storage device password is supplied in response to the access token reading device reading an access token and the input device receiving verification data;

storing a master password on the access token;

storing a nonvolatile storage device password on the access token; and

comparing the verification data to the master password and the nonvolatile storage device password for access to the computer system.

27. (Original) The method of claim 26 further comprising:

storing a password corresponding to the nonvolatile storage device password on the nonvolatile storage device.

28. (Previously Presented) A method for protecting information stored in an information handling system, said method comprising:

reading an access token containing a security policy for the information handling system;

requesting an authentication password from a user;

authenticating the use of the access token by comparing the password to the security policy;

setting a security policy in the information handling system; and

unlocking a nonvolatile storage device on the information handling system.

29. (Previously Presented) A method for assembling a computer system, said method comprising:

receiving a list of components for assembling the computer system;

receiving one or more security policies;

configuring the computer system using the one or more security policies; and

accessing the computer system with a user input password combined with a token access password such that the combined passwords match the one or more security policies configured in the computer system.

30. (Original) The method of claim 29 further comprising:

initializing a system password installed on the computer system.

31. (Original) The method of claim 29 further comprising:

providing a nonvolatile storage device for the computer system, wherein the nonvolatile storage device includes a nonvolatile storage device password; and

initializing the nonvolatile storage device password.

32. (Original) The method of claim 29 wherein the configuring includes modifying a nonvolatile memory installed in the computer system.

33. (Original) The method of claim 29 further comprising:

retaining a copy of the nonvolatile storage device password at a location removed from the computer system.

34. (Previously Presented) The method of claim 29 further comprising:

configuring an access token for the computer system, the access token including the security policies and the passwords associated with the computer system.

35. (Previously Presented) A method of using an access token, said method comprising:

transferring one or more passwords from the access token to a computer system;

receiving a user input password at the computer system; and

matching a computer system password with the user input password with the one or more passwords from the access token to access the computer system, wherein the computer system password includes one or more security policies configured in the computer system.

36. (Previously Presented) The method of claim 35 wherein the transferring step is performed in response to an access code received by the access token.

37. (Original) The method of claim 35 wherein one of the one or more passwords corresponds to a computer system password installed on the computer system.

38. (Original) The method of claim 35 wherein one of the one or more passwords corresponds to a nonvolatile storage device password installed on a nonvolatile storage device.

39. (Cancelled).

40. (Previously Presented) A communication device having an access token for use with a computer system, said communication device comprising:

one or more security policies adapted to be used by the computer system, wherein the one or more security policies are stored in an encrypted format; and

a security code stored on the access token, wherein the communication device transmits the one or more security policies in response to receiving an authentication code corresponding to the security code.

41. (Previously Presented) A computer operable medium for protecting a computer system, said computer operable medium comprising:

means for reading an access token containing a security policy for the computer system;

means for receiving an authentication password from a user;

means for verifying the validity of the access token based on a comparison of the authentication password to the security policy;

means for setting security policies in the computer system; and

means for unlocking a nonvolatile storage device on the computer system.

42. (Previously Presented) An information handling system comprising:

means for reading an access token containing a security policy for the information handling system;

means for receiving an authentication password from a user;

means for verifying the validity of the access token based on a comparison of the authentication password to the security policy;

means for setting security policies in the information handling system; and

means for unlocking a nonvolatile storage device on the information handling system.